IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

EQUIFAX, INC., Plaintiff Counterclaim-Defendant, v. VERID, INC., Defendant Counterclaim-Plaintiff.	)	Civil Action File No. 1:06-CV-2404-TCB

PLAINTIFF EQUIFAX, INC.'S OPENING CLAIM CONSTRUCTION BRIEF

William F. Long
Michael I. Krause
SUTHERLAND ASBILL & BRENNAN LLP
999 Peachtree Street, NE
Atlanta, GA 30309
Telephone: (404) 853-8000
Fax: (404) 853-8806

Attorneys for Plaintiff Equifax, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF EXHIBITS

Equifax, Inc. ("Equifax") hereby submits under Local Patent Rule 6.5 its opening brief in support of its constructions for the claim terms in dispute. A copy of Equifax's proposed constructions and Verid's proposed constructions are attached as Exhibits B and C, respectively.

I. THE '447 PATENT

The patent at issue is U.S. Patent No. 6,263,447 (the '447 patent"), issued on July 17, 2001. The patent is directed to a multi-level authentication system that can authenticate an individual over a network, or in other words, verify that the person is who he or she claims to be. The '447 specification explained the problems with prior art password based systems:

> Passwords provide some level of protection, but they are not fail-safe. One reason passwords are vulnerable is that users often share them. Even if they are kept private, someone who wants to obtain a password badly enough often can.... Moreover, when dealing with unknown users such as people who want to conduct an electronic transaction over the Internet, ad hoc passwords are not practical. [1:39-47].[1]

The specification further explained the problems with existing "one-level" authentication schemes:

> [A] user who provides accurate information [over a network] may not be authenticated... for example, because the user enters a nickname or a contraction rather than a proper name.... [A] user who supplies fraudulent information may be

[1] A copy of the '447 Patent is attached as Exhibit A. References to the '447 Patent appear in square brackets, *e.g.* [1:39-47] refers to column 1, lines 39-47.

> authenticated. … Both false positives and false negatives are undesirable. [1:57-2:5]

One object of the invention disclosed in the '447 Patent was "to overcome these and other drawbacks of existing authentication systems…." [2:11-12].

To address these problems, the '447 patent disclosed a novel multi-level user authentication scheme:

> The user is presented with a hierarchy of queries based on wallet-type (basic identification) and non-wallet type (more private) information designed to insure the identity of the user and prevent fraud [and] false negatives. [Abstract]

The Summary of the Invention explained that the invention may have one or more levels of authentication. At each level of authentication, personal information from the user is compared with information received from a reliable source to evaluate whether they match:

> Generally in the invention, the user is authenticated according to their ability to respond to successive queries for personal information and the level of match attained from comparing the information they provide with reliable data sources. [Summary of The Invention, 3:16-20]

Although the use of two or more levels are described as being preferable, the first level of authentication, which is based upon the user's "identification information," is mandatory:

> The user is initially requested to provide *a first type of identification information*. [3:20-21, emphasis added].

This first type of identification information is preferably "wallet-type" information:

> This first type of identification information is preferably wallet-type information, that is, information such as name, address, driver's license or other information that may be commonly carried on the person. This information is transmitted to the authentication server which carries out a first level authentication process on that information. [3:16-27].

The first level of authentication is performed by comparing the user's identification information (*i.e.,* the "first type of information") with reliable information about the user from a source other than the user:

> That first level authentication process compares the degree of match between the user-supplied first type of information and known data about the user from other sources. [3:27-31].

Preferred embodiments include systems with at least two levels of authentication. In those embodiments, the second level authentication is based upon a "second type of information" that is fundamentally different than the first type of information, namely non-wallet information, not carried on the person, that is more private in nature:

> Preferably, the second and any additional levels of authentication request a second, non-wallet type of information from the user. The second type of information is preferably based on comparatively private information that only the user would know.... Such information is typically not carried with a person, and therefore the chances of fraud by someone who obtains lost or stolen information and attempts to execute a transaction are reduced. [3:35-45]

As noted previously, the second and any subsequent levels of authentication, like the first level, include comparing the information from the user with information from reliable data sources other than the user:

> Generally in the invention, the user is authenticated according to their ability to respond to successive queries for personal information and the level of match attained from comparing the information they provide with reliable data sources. [3:16-20]

In one (but not all) of the disclosed embodiments, the second level of authentication "generates" a multiple choice question and answer set, with a single correct answer and multiple wrong answers. The correct answer depends upon what information about the user is "available" in the known data sources, with the correct answer (and therefore the question) being determined based on those sources:

> The … data elicited in the second level authentication process may be requested using an interactive query. The interactive query may include multiple choice questions that are automatically generated based upon the information available in the known data sources. For example, the authentication server may access a credit file to identify loans of the user which are still in payback status. One or more loans may be selected and the lender's name and corresponding monthly payment amount retrieved from the credit file. [3:45-55]

The specification describes other alternative features, some of which will be discussed in more detail below.

II. CLAIM TERMS SHOULD BE GIVEN THEIR PLAIN AND ORDINARY MEANING IN THE CONTEXT OF THE INTRINSIC EVIDENCE

"It is a 'bedrock principle' of patent law that the claims of a patent define the invention to which the patentee is entitled the right to exclude." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (citations omitted). Claim terms are generally given their ordinary and customary meaning, which is the meaning that the terms would have to a person of ordinary skill in the relevant art at the time of the invention. *Phillips*, 415 F.3d at 1312-13 (citations omitted). "Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification." *Id.* at 1313. Indeed, claims "must be read in view of the specification, of which they are a part." *Id.* at 1315 (citations omitted). The specification is usually "dispositive; it is the single best guide to the meaning of the disputed term." *Id.* at 1315 (citations omitted).

Although courts may refer to extrinsic evidence in some instances, which "consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises," extrinsic evidence cannot be used to contradict clear intrinsic evidence. *Id.* at 1317, 1318 (citations omitted).

III. EQUIFAX'S PROPOSED CLAIM CONSTRUCTIONS

Equifax requests the Court to adopt the following constructions for the disputed terms, as follows:

A. "authenticating a user on a network" (asserted claims 1, 9, 13, 17, 26, 34, 38 and 42)

The phrase "authenticating a user on a network" is used in all asserted independent claims, and the parties agree that "authenticating a user on a network" has the same meaning in all claims. Equifax proposes that this phrase means "proving or determining, to a sufficient level of certainty, whether or not an *individual* on a network is who the individual claims to be." Verid agrees with Equifax's construction, except that Verid apparently contends that the recited user authentication is not limited to authentication of a person, and could be some non-human user, such as a business, machine, or some other computer.

In the '447 specification, the word "user" refers exclusively to an individual, *i.e.,* a person. The patent describes "the invention" (as opposed to simply an embodiment of the invention) as being based upon "personal information." *See* Summary of The Invention ("Generally in the invention, the *user* is authenticated according to their ability to respond to successive queries for *personal* information…." [3:17-18, emphasis added]). The Abstract explains that the user is authenticated with "wallet-type (basic identification) and non-wallet type (more

private information)." Wallet-type refers to *personal* identification information such as name, date of birth, social security number, address, telephone number and driver's license, information that may be "commonly carried *on the person*." [1:50-55; 3:22-24; 13:3 (emphasis added)]. The reference to non-wallet type also reflects that the user is a person: "[T]he second and any additional levels of authentication request a second, non-wallet type of information from the user. The second type of information is preferably based on comparatively private information that *only the user would know*." [3:34-38 (emphasis added)]. Reference to what the user "knows" underscores that the user must be a person. *See, also* [18:63 – 19:5] ("In general, as illustrated in [Fig. 31],[2] the user presents name, social security number, date of birth, email and mailing address information, followed by home telephone number and driver's license data[.]"). "User" in this context refers to a person.

Verid's testifying authentication expert, Dr. Cranor, admitted that "user authentication" is a term of art in the authentication field that means "individual authentication" (Cranor Dep. at 38)[3] and that "individual authentication" means establishing that the identity being authenticated refers to a "specific individual." Cranor Dep. Ex. 5, chap 1, at p. 3 of 16 (*see* Ex. E). Dr. Cranor admitted that her

---

[2] The specification at this point actually refers to Fig.18. The reference to Fig. 18 is a typographical error. The correct and intended reference is Fig. 31. Cranor Dep. at 171-72.

[3] Excerpts of the deposition of Dr. Cranor are attached as Exhibit D.

construction of authenticating a user was "individual authentication," in which the system authenticates that a specific, unique person is the person he/she claims to be, and she admitted that her construction is inconsistent with "identify authentication," in which the system cannot tie the authenticated entity to a real person. Cranor Dep. at 38-41.

Nevertheless, following a break in the deposition, Dr. Cranor "clarified" that "I don't think that the patent actually precludes discussion of the other types of authentication mentioned here, although its focus is on individual authentication." Cranor Dep. at 43.

Saying merely that the "focus of the patent" is an individual authentication is a gross understatement; in fact, the entirety of the specification (including the Abstract and the Figures) make clear that "user" means a real person, an individual consumer. The only suggestion within the entire patent that the disclosed system theoretically could be used for a non-person is in the final paragraph of the specification, stating as an afterthought that the system "can also verify the identity of other entities such as corporations, schools, government units and others seeking to transact business over a network." [21:19-26] However, this final paragraph distinguishes the term "user," which the patent describes as referring to an individual consumer: "the invention has been [up to this point] illustrated in terms of an *individual consumer* initiating a network transaction…." 21:19-21 (emphasis

added). Although it references in passing that the system could theoretically be applied to non-humans, this final paragraph does not refer to such non-human entities as "users," does not suggest that corporate or business authentication of a non-human entity would constitute "user authentication," and does not disclose how to accomplish such non-human authentication. The patent describes no embodiment of a system to authenticate a non-human.

Accordingly, "authenticating a user on a network" means "proving or determining, to a sufficient level of certainty, whether or not an *individual* on a network is who the individual claims to be."

B. "first type of information" [asserted claims 1, 9, 13, 17, 26, 34, 38 and 42]

The phrase "first type of information" appears in all asserted independent claims. The phrase means "a category of information comprising personal identification information, such as name, social security number, address, telephone number, driver's license number, email address and other such personal identification information." There are three aspects to Equifax's construction: (1) the meaning of this phrase is the same for all claims; (2) "type" means "category"; and (3) first type of information must be "user identification information." These are discussed in the following.

1. "First type of information" possesses the same meaning in all claims.

The parties agree that "first type of information" possesses the same meaning for all claims. Dr. Cranor agrees. *See* Cranor Dep. at 121-122.

2. "Type" means "category."

Equifax's proposed definition clarifies that in the context of the claims, "type" means "category." Verid's expert agrees with Equifax that in the context of the '447 patent, "type" means "category." Cranor Dep. at 119-120.

In the context of the '447 patent, "type of information" means a category of information, or in other words, a grouping of information sharing common characteristics. (The patent provides for example, the category of "wallet-type" and another category of "non-wallet type." *See, e.g.,* Abstract. Outside the context of the '447 patent, "type of information" is more ambiguous: it could mean a category of information, or it could mean simply an example of information (*e.g.,* "the first example of information and the second example of information") or it could have other meanings.

Verid has not explained why it does not accept "category" as the proper definition of "type." Equifax therefore requests the Court to construe the term in accordance with its plain meaning now to prevent the parties from later disputing the meaning of "type."

3. "First type of information" means "user identification information."

Equifax's construction flows from the plain language of the claims. As noted above, the system relies upon the "first type of information" to perform the first authentication step. Independent claims 9 and 34 state that "the first type of information supplied by the user is compared with the *user identification information* retrieved from the data source." [22:16-18; 24:43-45]. Dr. Cranor admits that an authentication step must be comparing, so to speak, "apples to apples." Cranor Dep. at 104-105. In other words, the information from the reliable data source used to compare the information from the user must be the same as the information received from the user, else the comparison will be useless. Because the first type of information received from the user is compared in claims 9 and 34 to "user identification information" from the reliable data source, the first type of information from the user must also be user identification information.

As Verid and Dr. Cranor agree, "first type of information" means the same in all independent claims. Claims 9 and 34 therefore make clear that "first type of information" means "user identification information" in all claims.

The specification further supports Equifax's construction. In describing the invention generally, the Summary of the Invention defines the first type of information to be "identification information:"

> Generally in the invention, the user is authenticated according to their ability to respond to successive queries for personal information and the level of match attained from comparing the information they provide with reliable data sources. The user is initially requested to provide *a first type of identification information*. [3:16-22 (emphasis added)].

Again in column 6, the specification equates the first type of information to "user identification information: "Authentication process 10 invokes the preprocessing step 26, in which the user is prompted to supply *a first type of user identification information*. [6:18-24 (emphasis added)].

Verid proposes that first type of information means "different types of information." Verid states that "the patent indicates that the "first type of information" and "second type of information" can come from different data sources, or that one can be public information and the other essentially private information…." Verid overlooks that the specification distinguishes "information" and "data source." A given type of information can come from more than one data source, and hence, merely changing the data source does not necessarily change the type of information. *See, e.g.,* [19:26-31]; *see also* Cranor Dep. at 117.

Verid overlooks that the '447 Patent specifically defines the first information as user identification information. [3:16-22 ("user is initially requested to provide a first type of identification information"); 6:18-24 ("user is prompted to supply a first type of user identification information")]. Verid's construction also ignores

that claims 9 and 34 *require* the first type of information to be "user identification information." [22:16-19; 24:46-49 (comparing "first type of information supplied by the user" with "user identification information retrieved from the data source")].

The Court should therefore construe "a first type of information" to mean "a category of information comprising personal identification information, such as name, social security number, address, telephone number, driver's license number, email address and other such personal identification information."

C. "perform[ing] a first authentication [step]" [asserted claims 1, 9, 13, 17, 26, 34, 38 and 42]

The phrase "perform (or performing) a first authentication (or first authentication step) based on a first type of information" appears in all asserted independent claims (1, 9, 13, 17, 26, 34, 38 and 42). Equifax proposes that the phrase means "verifying (or verify) that a person is who he or she claims to be by comparing the first type of information received from the person with information received from a reliable data source other than the person." This construction includes three aspects: (1) authentication requires a comparison; (2) the comparison must be with "reliable" non-user sources; and (3) the system "verifies" the accuracy of the information as a result of the comparison. As explained in more detail below, Equfiax's proposed construction is consistent with the plain

meaning of the term "authenticate" as used in the specification and as confirmed by Dr. Cranor.

1. Authentication requires a comparison of information from the user with information about the user from some other source.

The Summary of the Invention, and indeed, all portions of the specification, define the first authentication step as a comparison of user-supplied information with information from other sources:

> This information [*i.e.,* identification information] is transmitted to the authentication server which carries out a first level authentication process on that information. That first level authentication process compares the degree of match between the user-supplied first type of information and known data about the user from other sources. [3:24-31]

The first level authentication comparison is reiterated in the preferred embodiment description:

> Authentication process 10 matches, at step 32, the first type of information input by the user with information received from one or more separate data sources. Based on that comparison, authentication process 10 determines whether the first level authentication is complete…. [13:21-25].

Figure 2 also shows that the first level authentication is a comparison, *see* Fig. 2 (at step 52, "First Level Comparing"), and the specification explains that "The first level comparing step 52 compares the information input by the user with

information about the user retrieved from one or more known data sources." [13:52-54 and Fig. 2].

Verid's expert agrees that "authentication" inherently requires comparison of information received from the user with the same information about the user from some other source that the system believes to be reliable. Dr. Cranor was not able to provide even an example of authentication that would not encompass such a comparison. *See* Cranor Dep. at 95, 98-99, 104.

2. The non-user source of information about the user must be "reliable."

The data sources used for the authentication comparison must be reliable. The Summary of the Invention section explains that "[g]enerally in the invention, the user is authenticated according to their ability to respond to successive queries for personal information and the level of match attained from comparing information they provide with *reliable* data sources." [3:16-20 (emphasis addes); *see also* 3:27-30 ("That first level authentication process compares the degree of match between the user-supplied first type of information and *known data* about the user from other sources.")(emphasis added); 3:47-50 ("The interactive query may include multiple choice questions that are automatically generated based upon the information available in the *known data sources*.") (emphasis added); 13:52-54 ("The first level comparing step 52 compares the information input by the user

with information about the user retrieved from one or more *known data sources.*") (emphasis added)]. Dr. Cranor agrees that in an authentication process, the non-user supplied data source relied upon to authenticate a user must be a reliable source of data. Cranor Dep. at 99.

3. The authentication comparison "verifies" the information received from the user.

Equifax has proposed the word "verifying" in the context of this phrase, because "verification" is the term used, for example, in the Abstract. Verid has proposed "proving or determining." Dr. Cranor agrees that verifying means the same as "proving or determining." See, e.g., Cranor Dep. at 22-24, 28-30. Hence, it appears that the parties' proposed constructions for the authentication "verb" are essentially the same. However, "verifying" provides a more compact construction than "proving or determining." Furthermore, the Abstract of the '447 Patent refers to "verification." Hence, "verifying" or "verify" provides the better construction.

The Court should therefore construe "perform [or performing] a first authentication step based on a first type of information" to mean "verifying [or verify] that a person is who he or she claims to be by comparing the first type of information received from the person with information received from a reliable data source other than the person."

D. "second type of information other than the first type of information" [asserted claims 1, 9, 13, 17, 26, 34, 38 and 42]

The phrase "second type of information other than the first type of information" appears in all asserted independent claims. The plain language of this phrase means that the second type of information must be of a type other than the first type of information. As noted above in the discussion of "first type of information," "type" means category. Hence, the second category of information must not merely be different from the first information, it must be in a different category than the first information.

For example, the specification provides examples of first and second categories of information, namely, wallet type and non-wallet type. If the first type of information is wallet-type, such as, for example, a social security number and date of birth, then the second information cannot be something merely different than a social security number and date of birth. The second type of information must be non-wallet type, which means it must be different not only from social security number and date of birth, but it also must be different than any wallet-type information. It must be non-wallet type information.

Verid's proposed construction could be interpreted to mean that the second information is only required to be different from the first information. The claim limitation expressly requires that the second information be not only different from the first, but must also be in a completely different category than the first.

The Court should therefore construe the phrase "second type of information other than the first type of information" to mean "a second category of information other than the first category of information".

E. "perform[ing] a second authentication [step]" [asserted claims 1, 9, 13, 17, 26, 34, 38, and 42]

All asserted claims include the phrase "perform at least a second authentication step (or second authentication) based on a second type of information. "Equifax's proposes that this phrase be construed as "after the first authentication step at least verifying (or verify) that the person is who he or she claims to be by comparing the second type of information received from the person with information received from a reliable data source other than the person." There are two aspects to this construction: (1) the second authentication step must follow the first authentication step, and (2) the second authentication step, like the first authentication step, involves a comparison of information from a reliable non-user source.

1. Second authentication is performed after the first authentication.

The plain language of "First" and "Second" authentication steps connote that the "second" step is after the first step: *i.e.,* first is before second. In independent claims 9 and 34, the second authentication step is based upon information from the

first authentication step: "performing a second authentication step … wherein the data source for the first type of information is used to identify the availability of the second type of information." [22:23-27; 24:50-55]. Hence, in the context of the claims, the second step must follow the first.

The specification confirms that the second step follows the first step. The invention consists of "successive queries for personal information." [3:17-18]. "At the completion of this first level authentication, the process … may proceed to another level of authentication." [3:31-33; *see also* 3:35 ("second and any additional levels of authentication"]. That the second level authentication follows the first level authentication is depicted in Fig. 1, a flowchart of the overall processing of the system. [5:28-32; 13:31-35]. Dr. Cranor, Verid's expert, agrees that the second authentication step must be after the first. Cranor Dep. at 146.

2. Second authentication step involves comparing information from the user with reliable information from a non-user source.

The Summary of the Invention explains that, like the first authentication step, the second authentication step compares information from the user with information from reliable data sources. [3:16-20; 34-63].[4] The difference between

[4] Although the use of a second authentication level is described in the Summary of the Invention as a preferred embodiment, the claim language makes indisputable that the claims are intended to cover the embodiment in which at least two authentication steps are used.

the first and second authentication is that the second is conducted after the first, and the second is based upon a comparison of a different category of information than is used in the first authentication step. *Id.*; *see also* [13:35-38] ("[Second level authentication] Step 40 request and tests the user's input of a second type of information…."); [14:51-58 and Fig. 3] ("Fig. 3 is a flowchart illustrating the second level authentication process 40 in more detail. Second level authentication process 40 begins with step 310. Step 310 accesses available second type of information from data sources, such as a credit file. Step 312 prompts the user for second type information from within that determined to be available at step 310. Step 314 determines whether the user input matches the accessed information.").

As noted above, Dr. Cranor confirmed that an authentication step involves comparing information from the user with reliable information from a source other than the user. Cranor Dep. at 98-99.

3. Verid's construction is not supported by the plain language of the claim or the specification.

Verid' s construction requests the court to require that the second authentication be conditional: "*If* the first authentication is unable to authenticate a user with a sufficient level of certainty, performing at least a second authentication…." (emphasis added). Verid thereby requests the court to improperly import a conditional requirement which is not required by the

specification and not supported by the plain language of the claims. Although some of the embodiments describe the second authentication step as being only a conditional step, that is not the only embodiment. For example, the summary of the invention states that "In an illustrative embodiment of the invention, a user who wishes to apply for an online transaction accesses a client/server network through a client terminal…. [T]he authentication server determines whether the user's identify can be confirmed, and the level of authentication that may be accorded to the user's identity based on rules specific to the vendor accepting the transaction…. *A greater level of security could conceivably be attained by automatically performing a thorough authentication process for every transaction.*" [2:47 – 3:11] (emphasis supplied). The plain language of the claims would encompass a system that performs both the first and the second authentication steps. An authentication when the second step is not performed would not infringe the plain language of the asserted claims of the '447 Patent.

Dr. Cranor admitted that the plain language of the claims does not support an interpretation that the second authentication step is conditional. Cranor Dep. at 147-150.

The Court should therefore construe "perform (or performing) at least a second authentication step based on a second type of information other than the first type of information" to mean "after the first authentication (authentication

step) at least verifying (or verify) that the person is who he or she claims to be by comparing the second type of information received from the person with information received from a reliable data source other than the person."

F. "generating [or generates] an interactive query..." [claims 1 and 26]

The phrase "generating (or generates) an interactive query, the interactive query comprising at least one question having multiple-choice answers wherein only one of the answers is the correct answer" appears in claims 1 and 26. Equifax proposes that this phrase means "bringing (or brings) into existence an interactive query comprising at least one multiple choice question having multiple-choice answers and a single correct answer."

The plain meaning of the term "generates" means "bringing into existence," i.e., "creates." Dr. Cranor agrees that at least one plain language meaning of generating is bringing into existence. Cranor Dep. at 130.

The claim refers to the "generation" of an interactive query. The Summary of the Invention, which provides the only use of the word "generated" in describing the interactive multiple choice query, uses the word "generated" to connote *dynamic creation*: "The interactive query may include multiple choice questions that are automatically *generated* based upon the information available in the known data sources." 3:48-50 (emphasis added). Dr. Cranor admitted that this

portion of the specification means that the multiple choice questions "are developed through an automatic process specifically for the user that's being authenticated currently." Cranor Dep. at 134. In other words, generated means created.

Another portion of the specification describes the interactive query as being "dynamically created," which further confirms that "generated" means "bringing into existence." [18:36-39 ("If the user is available at the time of application for an interactive dialog (e.g., Internet request), a multiple choice questionnaire is preferably *dynamically created* by authentication process 10 and presented to the user, through client 110, for completion.") (emphasis added)]. Dr. Cranor admits that this portion of the specification refers to something that "is created in real time." Cranor Dep. at 137.

Verid and Dr. Cranor argue that "generating a query means simply *presenting* such an inquiry to the user." Equifax does not dispute that the interactive query must be presented to the user, but "generating" does not mean "presenting," in any context, especially not in the context of the '447 Patent.

The '447 specification distinguishes the "presenting" function from the "generating function." For example, the interactive query is "dynamically created." [18:38]. Not until *after* the query is dynamically created can it then be "presented to the user." [18:39]. The '447 patent distinguishes between the meaning of

"presenting" and "generating" in other contexts. For example, in one embodiment, the system can create a digital certificate following successful authentication. The digital certificate being created is referred to as being "generated." [19:12]. This contrasts with the explanation in the same paragraph that the interactive query is "presented." [19:7; *see, also,* 2:63-65 ("Once the authentication process has been satisfied, the invention may *generate* a digital certificate.... The digital certificate can then be *presented* in future transactions ....") (emphasis added)]. In sum, the patent uses "generate" and "present" distinctly differently: generate means "create," not "presenting to the user."

The Court should therefore construe "generating (or generates) an interactive query, the interactive query comprising at least one question having multiple-choice answers wherein only one of the answers is the correct answer" to mean "bringing [or brings] into existence an interactive query comprising at least one multiple choice question having multiple-choice answers and a single correct answer."

G. "determining a level of correspondence ..."

The phrase "determining a level of correspondence between the first type of information supplied by the user and the user identification information retrieved from the data source" as used in claims 9 and 34 means "ascertaining the degree of

match between the first type of information supplied by the person and information received from the data source other than the person."

Equifax's proposed construction is based upon the specification, which states: "That first level authentication process compares the degree of match between the user-supplied first type of information and known data about the user from other sources." [3:27-31]. Dr. Cranor agreed that Equifax's proposed construction was a fair construction of this limitation. Cranor Dep. at 144-145.

Therefore, the Court should construe "determining a level of correspondence between the first type of information supplied by the user and the user identification information retrieved from the data source" to mean "ascertaining the degree of match between the first type of information supplied by the person and information received from the data source other than the person."

H. "identify the availability of the second type of information..." [claims 9 and 34]

Claims 9 and 34, respectively, each include the phrase "identify the availability of the second type of information...." This phrase is best understood in the context of the specification, which describes an embodiment in which the second authentication step is based upon a second type of information that is determined to be "available." The embodiment is first described in the Summary of the Invention:

> That first level authentication process compares the degree of match between the user-supplied first type of information and *known data about the user from other sources*. … The interactive query [of the second authentication step] may include multiple choice questions that are automatically generated *based upon information available in the known data sources*. [3:27-50 (emphasis added)].

The embodiment is similarly described in the description of the second authentication step:

> Second level authentication process 40 begins with step 310. Step 310 accesses *available second type information* from data sources, such as a credit file. Step 312 prompts the user for second type information from within that *determined to be available* in step 310. [14:51-15:16 (emphasis supplied)].

Thus, the second type of information can be selected from information determined to be "available" in known data sources.

The second information used for the second authentication step is not "determined" until *after* the first authentication step, and is selected based upon what information is "available" in the known data sources that were used in the first authentication step. In Figure 3, therefore, the authentication step *first* accesses the second type information (from the data source used in the first authentication step), *then* it prompts the user for that information. Figure 3 shows that in this embodiment, the system does not first prompt the user for information because it cannot do that until it determines what second type of information is available.

The remainder of the claim language in claims 9 and 34 is self-explanatory. In claim 9, the phrase "*the data source for the first type of information* is used to identify the availability of the second type of information for the user" makes clear that "the data source for the first type of information" is used to determine what information is available to use for second level authentication. The language of claim 34 is quite similar to claim 9, except that claim 34 uses "user identification information retrieved from the data source" to identify what second information is available. "Step 310 accesses available second type information from data sources, such as a credit file." [14:52-55].

Verid's proposed construction includes "potential data source." However, the second information is chosen from what is *actually* available, not what is potentially available. For example, second level authentication questions are generated "based upon *information available* in the data sources" – not information "potentially" available. [3:49-50 (emphasis added)]. Similarly, "[s]tep 310 accesses available second type information," not a "potentially" available data source. [14:53-55].

The Court should therefore adopt Equifax's proposed constructions for claims 9 and 34. The phrase in claim 9 means "wherein the data source for the first type of information is used to identify what second type of information about the person is available for implementing the second authentication step." The

phrase in claim 34 means "wherein the first type of information retrieved from the data source is used to identify what second type of information about the person is available for implementing the second authentication step."

I. "executes a pattern recognition process ..."

The phrase "executes (or executing) a pattern recognition process to detect potential irregularities in at least one of the first type of information and the second type of information" as used in claims 17 and 42 means "analyzes (or analyzing) either or both of the first and second type of information, received in repetitive attempts to authenticate, to detect a pattern of irregularities, for example, a pattern suggesting fraud."

The specification explains: "An illustration of pattern recognition criteria that may be employed in this regard by the invention is illustrated in FIGS. 17 and 18. As illustrated in those figures, in general the invention monitors user input recorded in transaction record 112 or otherwise for *repetitive attempts at authentication*, which may represent attempted fraud or some type of network attack." [11:51-64 (emphasis added)]. The pattern being analyzed is a pattern that can only exist over multiple attempts to authenticate.

Therefore, the proper construction of "executes [or executing] a pattern recognition process to detect potential irregularities in at least one of the first type

of information and the second type of information" is "analyzes [or analyzing] either or both of the first and second type of information received from the person to detect a pattern of irregularities".

IV. CONCLUSION

For all the foregoing reasons, Equifax respectfully requests that the Court adopt its proposed claim constructions regarding the terms of the '447 patent as set forth herein.

DATED:

SUTHERLAND ASBILL & BRENNAN LLP

/s/ William F. Long

William F. Long (Georgia Bar No. 457490)
Michael I. Krause (Georgia Bar No. 429286)
999 Peachtree Street, NE
Atlanta, GA 30309
Telephone: (404) 853-8000
Fax: (404) 853-8806
Email: bill.long@sablaw.com
Email: michael.krause@sablaw.com

Attorneys for Plaintiff Equifax, Inc.

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

EQUIFAX, INC.,	)	
	)	
Plaintiff,	)	
	)	Civil Action No. 1:06-CV-2404-TCB
v.	)	
	)	
VERID, INC.,	)	
	)	
Defendant.	)	

CERTIFICATE OF SERVICE

I hereby certify that I have, this day, served a true and correct copy of the within and foregoing **PLAINTIFF EQUIFAX, INC.'S OPENING CLAIM CONSTRUCTION BRIEF** on counsel for Defendant via electronic mail as follows:

Jeffrey C. Morgan (Georgia Bar No. 522667) Bank of America Plaza, Suite 5200 600 Peachtree Street, N.E. Atlanta, GA 30308 Telephone: (404) 885-3000 Fax: (404) 885-3900 Email: jeffrey.morgan@troutmansanders.com	William F. Lee (*Admitted Pro Hac Vice)* Cynthia Vreeland (*Admitted Pro Hac Vice)* 60 State Street Boston, MA 02109 Telephone: (617) 526-6000 Fax: (617) 526-5000 Email: william.lee@wilmerhale.com Email: cynthia.vreeland@wilmerhale.com

Mark Rienzi (*Admitted Pro Hac Vice)* 1875 Pennsylvania Avenue, NW Washington, DC 20006 Telephone: (202) 663-6000 Fax: (202) 663-6363 Email: mark.rienzi@wilmerhale.com	Alexandra McTague (*Admitted Pro Hac Vice)* 399 Park Avenue New York, NY 10022 Telephone: (212) 230-8800 Fax: (212) 230-8888 Email: alexandra.mctague@wilmerhale.com

Dated this 17th day of September, 2007.

/s/ Michael I. Krause
Michael I. Krause

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

EQUIFAX, INC.,	)	
	)	
Plaintiff,	)	
	)	Civil Action No. 1:06-CV-2404-TCB
v.	)	
	)	
VERID, INC.,	)	
	)	
Defendant.	)	

CERTIFICATE OF COMPLIANCE

Pursuant to Local Rule LR 7.1D, I hereby certify that the foregoing "Plaintiff Equifax, Inc.'s Opening Claim Construction Brief" complies with the relevant font and point selection limitations of Civil Local Rule LR 5.1B. This brief is typed in Times New Roman (14 point) according to the word-processing system used to prepare it.

/s/Michael I. Krause
Michael I. Krause
Attorney for Plaintiff